

# Digitalno upravljanje autorskim pravima

---

**Miličević, Leon**

**Undergraduate thesis / Završni rad**

**2018**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Pula / Sveučilište Jurja Dobrile u Puli**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:137:777973>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2025-01-04**



*Repository / Repozitorij:*

[Digital Repository Juraj Dobrila University of Pula](#)



Sveučilište Jurja Dobrile u Puli  
Odjel za informacijsko komunikacijske-tehnologije

**LEON MILIČEVIĆ**

**DIGITALNO UPRAVLJANJE AUTORSKIM PRAVIMA**

Završni rad

Pula, 2018.

Sveučilište Jurja Dobrile u Puli  
Odjel za informacijsko komunikacijske-tehnologije

**LEON MILIČEVIĆ**

**DIGITALNO UPRAVLJANJE AUTORSKIM PRAVIMA**

Završni rad

JMBAG: 0303038293, redovan student  
Studijski smjer: preddiplomski studij Informatika  
Kolegij: Multimedijalni sustavi  
Mentor: doc. dr. sc. Darko Etinger

Pula, Ožujak 2018.



## IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani \_\_\_\_\_ kandidat za prvostupnika \_\_\_\_\_ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mogega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to prikazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da ni jedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

\_\_\_\_\_

U Puli, \_\_\_\_\_, \_\_\_\_\_ godine.

## Sadržaj

UVOD.....	1
1. INTELEKTUALNO VLASNIŠTVO .....	2
2. DEFINICIJE, STAJALIŠTA I PREGLED DRM-a .....	3
2.1. KAKO DRM FUNKCIONIRA .....	6
2.2. AUTORSKO PRAVO - COPYRIGHT .....	7
2.3. DIGITALNE BRAVE .....	8
2.4. OKVIR DRM-a .....	9
2.5. RIGHTS EXPRESSION LANGUAGE .....	11
2.6. PRIMJER PRIMJENE DRM-A .....	11
3. ULOGA DRM TEHNOLOGIJA NA TRŽIŠTU DIGITALNIH SADRŽAJA.....	14
3.1. TRŽIŠNE POSLJEDICE UPOTREBE DRM TEHNOLOGIJA .....	14
3.2. DRM KAO RIZIK ZA TRŽIŠNO NATJECANJE.....	15
4. IMPLEMENTACIJA DRM-A U RAZLIČITIM VRSTAMA AUTORSKIH DJELA	17
4.1. DOKUMENTI.....	17
4.2. FILM.....	19
4.3. E-KNJIGE .....	21
4.4. RAČUNALNE IGRE .....	23
4.5. GLAZBA .....	26
4.6. SERVISI ZA STRUJANJE MULTIMEDIJKOG SADRŽAJA.....	29
ZAKLJUČAK.....	31
LITERATURA .....	33

## UVOD

Digitalno upravljanje autorskim pravima (engl. Digital Rights Management – DRM), predstavlja razne metode upravljanja i zaštite autorskih prava u digitalnom obliku, koje se služe tehnologijama kontrole pristupa, kako bi ograničili uporabu djela zaštićenih autorskim pravom. DRM tehnologije pokušavaju kontrolirati korištenje, modifikacije, te distribuciju autorskih djela kao što su softver ili multimedijalni sadržaji (filmovi, glazba, slika, knjige, igre, dokumenti) kao i sustave unutar tih uređaja koji provode tu politiku zaštite. Općenito, kontrola pristupa je selektivno ograničavanje pristupa nekome ili nečemu do nekog mjesta (fizičkog) ili drugog izvora (digitalnog na primjer).

Korištenje DRM-a nije univerzalno prihvaćeno – neki ga ne prihvaćaju, a neki ga prihvaćaju i žele sprovesti. Zagovornici DRM-a tvrde da je nužno zaštititi intelektualno vlasništvo od slobodnog kopiranja i distribucije. Poput fizičkih lokota koji imaju ulogu spriječiti osobnu imovinu od krađe, treba postojati način i za zaštititi djela vlasnika autorskih prava kako bi održali tzv. Artistic control<sup>1</sup>, te si osigurali kontinuirani priljev prihoda koji ostvaruju od svog djela.

Ovaj rad će govoriti o zaštiti autorskog prava koje je srodno s intelektualnim vlasništvom. Stoga, prvo ću predstaviti osnovne definicije i pojmove intelektualnog vlasništva, autorskog prava, DRM-a, te zatim prijeći na tehnologije, odnosno medije koji se zaštićuju, te načine zaštite, koje će biti okrijepljene primjerima iz prakse. Kroz rad ću davati primjere kako je neki sustav zaštite dobra opcija, no i zbog čega je loša. Te zaključiti subjektivnom misli o ovoj temi.

---

<sup>1</sup> Artistic control je izraz koji se najčešće koristi kod filmova i glazbe, gdje će uvijek postojati neka posredna osoba poput producenta koji će modificirati proizvod, no umjetnik, odnosno osoba koja ima artistic control, ima pravo odlučiti kako će izgledati konačni proizvod.

# 1. INTELEKTUALNO VLASNIŠTVO

Intelektualno vlasništvo odnosi se na proizvode stvorene ljudskim umom i pripadaju nematerijalnim dobrima. Njihova je vrijednost u umnožavanju, upotrebi i prikazivanju drugim ljudima, što sugerira da nije s jedne strane niti svrhovito, a s druge nije ni moguće zaštititi sakrivanjem, zatvaranjem ili drugim mjerama fizičke zaštite. Takva materijalna dobra imaju društvenu vrijednost i plod su rada, te ljudskog intelekta, pa ih je sukladno tome potrebno zaštititi od neovlaštenog korištenja. Takva dobra pripadaju njezinom stvaratelju, te pod određenim uvjetima predstavljaju njegovo intelektualno vlasništvo. Iako je neopipljivo u fizičkom smislu, intelektualno vlasništvo se može kupiti, licencirati, zamijeniti, pokloniti ili naslijediti kao i svako drugo vlasništvo. Stoga, u poslovnom smislu intelektualno vlasništvo predstavlja nematerijalnu imovinu čije uspješno iskorištavanje može biti vrijedan temelj ili doprinos poslovanju. Kako bi se ohrabrilo stvaranje inovacija i potaknula ljudska kreativnost koja doprinosi općem društvenom razvitku zemlje, razvijen je odgovarajući sustav pravne zaštite intelektualnog vlasništva koji odgovarajućim instrumentima uređuje način stjecanja intelektualnog vlasništva i način zaštite od njegovog neovlaštenog korištenja. [Državni zavod za intelektualno vlasništvo. URL: <http://www.dziv.hr/hr/intelektualno-vlasnistvo/o-intelektualnom-vlasnistvu/> (26.02.2018.) ].

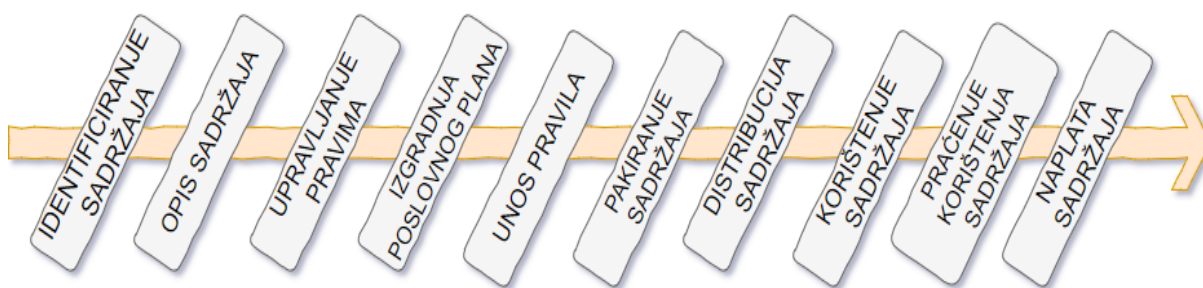
Intelektualno vlasništvo se dijeli na autorsko pravo i srodna prava koja se u načelu ne štite registracijom i priznaju se kao prava činom nastanka, prava industrijskog vlasništva (žig, industrijski dizajn, patent, oznaka zemljopisnog porijekla i oznaka izvornosti) i neformalno industrijsko vlasništvo (recepture, procesi, podaci) koje se ne štiti, ali je važno za očuvanje vrijednosti koje se stvaraju unutar poslovnog sustava.

Osnovna svrha zaštite intelektualnog vlasništva jest mogućnost dobivanja tržišnog monopola, te zarađivanja na vlasništvu određeno vrijeme u zamjenu za otkrivanje izuma i obogaćivanje ukupno evidentiranog ljudskog znanja. [Genius Croatia, baza ideja, izuma i inovacija iz Hrvatske, URL: <http://genius-croatia.com/info/pitanja-i-odgovori/> (26.02. 2018.) ].

## 2. DEFINICIJE, STAJALIŠTA I PREGLED DRM-a

Upravljanje digitalnim pravima (DRM) je vrsta poslužiteljskog softvera razvijenog kako bi se omogućila sigurna distribucija - a možda još važnije, onemogućila ilegalna distribucija - plaćenog sadržaja putem interneta.

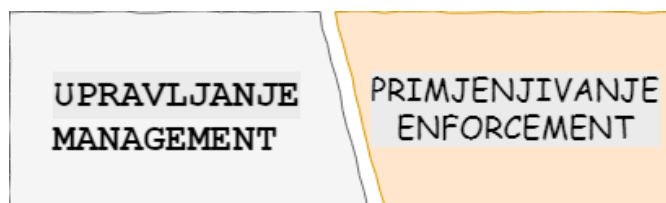
Iako je ova definicija definitivno istinita i predstavlja prilično dominantan pogled na ono što DRM jest i pruža, ne daje potpunu sliku jer izostavlja pogled u okruženje u kojemu će se koristiti. Dijagram sa slike 1. prikazuje okruženje pružajući korake koje većina sadržaja prolazi kada se njima trguje: Proizvodnja, digitalizacija, identifikacija, pripisivanje opisa, distribucija, uporaba (od strane potrošača), praćenje korištenja, te naplata.



Slika 1 Okruženje u kojemu se koristi DRM

Bilo koji od ovih koraka može se izostaviti u određenim okolnostima. Na primjer, ako se sadržaj distribuira besplatno - korak naplate neće se morati izvršiti.

DRM pokriva opis, identifikaciju, trgovanje, zaštitu, nadgledanje i praćenje svih oblika korištenja nad materijalnom i nematerijalnom imovinom. Također DRM možemo podijeliti na dva opća činitelja. Upravljanje (engl. management) te primjenjivanje (engl. enforcement) pravila.



Slika 2 Dva opća činitelja DRM-a Izvor:

Prikazano na slici 2, okvir upravljanja nam govori kako nositelji prava trebaju identificirati sadržaj kao svoj (kako bi vlasnik sadržaja znao koja prava uistinu posjeduje), prikupiti meta-podatke (kako bi potencijalni korisnici sadržaja mogli



pronaći isti), utvrditi prava koja se odnose na sadržaj (tek nakon toga moguće je pokušati distribuirati sadržaj), te razviti poslovne modele za distribuciju imovine. Okvir primjenjivanja određuje provedbu pravila eksploatacije koja određuje nositelj prava (ili bilo koji od poslovnih partnera nositelja prava, kao što su distributeri, trgovci na veliko, e-prodavači, itd.).

Najopćenitija definicija meta-podataka (engl. Metadata) kao podataka o podacima, temeljena je na etimologiji same riječi. Devedesetih godina prošlog stoljeća strukovne zajednice daju svoje definicije. Tako primjerice, World Wide Web Consortium meta-podatke definira kao strojno čitljive informacije za web. [Metadata at W3C. URL: <https://www.w3.org/Metadata/> (10.03.2018.)]

Osim stvarnog sadržaja, DRM izvlači i održava meta-podatke, koji se odnose na informacije o sadržaju. Ono sadrži informacije poput tipa sadržaja, ID sadržaja, detaljima o šifriranju, te informacije o pravima. Meta-podaci mogu biti klasificirani kao sadržajno opisni meta-podaci, te meta podaci ovisni o sadržaju. Sadržajno opisni meta-podaci sadrže informacije kao što su format podataka, format izgleda, razne komponente od kojih je sadržaj izrađen, te informacije o autoru sadržaja. Meta-podaci ovisni o sadržaju sadrže informacije koje se odnose na ono što je u sadržaju, poput ključnih riječi (engl. keywords). Meta-podaci koriste kako bi se lociralo sadržaj te nadziralo iskorištavanje sadržaja. [Subramanya, S.R. & Yi, B.K.. (2006). Digital rights management.]

DRM softver iskorištava meta-podatke tako da primarno prikuplja informacije poput imena kupca, informacije o računu ili adresu e-pošte. Također informacije o izdavaču, autoru, datumu izrade datoteke (ili stream-a ako se radi o prijenosu videa ili glazbe u živo), datumu preuzimanja datoteke, i razno razne bilješke. Te informacije se ne reproduciraju sa sadržajem poput vodenog žiga, ali se čuva zasebno, unutar datoteke ili mrežnog strujanja (engl. Stream)<sup>2</sup>. [Digital Rights Management, URL: [https://www.researchgate.net/publication/3227866\\_Digital\\_rights\\_management](https://www.researchgate.net/publication/3227866_Digital_rights_management) (30.11.2017.)]

---

<sup>2</sup> Live stream je generički naziv za tehnologiju prijenosa *streaming audio* i *streaming video*. Ova tehnologija je najpoznatija i kao web-radio i web-tv. Live stream označava prijem i istovremeno reproduciranje audio i video podataka putem računalne mreže. S toga je streaming media ekvivalent klasičnim prijenosu radijskog i televizijskog programa. Streaming media može se biti u živo (Internet TV ili radio) ili u kao ponuda emisija na zahtjev.

Dvije metode koje se koriste u borbi protiv piratstva su šifriranje (engl. Encryption) i vodeni žig. Šifriranje daje primarnu zaštitu. Ako je šifriranje ugroženo, vodeni žig omogućuje praćenje mogućih izvora piratstva.

Digitalni vodeni žig (engl. Watermark) termin je koji se koristi u računalnoj znanosti, kriptografiji, digitalnoj obradi signala i komunikacijama. Svrha postojanja ovog novog područja je omogućiti zaštitu multimedijских dokumenata u smislu autorskog prava, zaštite kopiranja (engl. Copyright protection) i sl. Postupak digitalnog označavanja temelji se na umetanju podatka, vodenog žiga, u izvorni dokument u svrhu njegove ponovne detekcije. Dokument koji se označava može biti bilo koja vrsta informacije: multimedijски dokument, video, slika, zvuk, tekst i sl. Žig može sadržavati bilo koju informaciju, kao na primjer identifikaciju kupca, prodavača ili nešto drugo. Algoritam ili shema koja opisuje postupak označavanja dokumenata digitalnim žigom sastoji se od tri komponente:

1. vodeni žig,
2. koder – algoritam korišten za umetanje žiga te
3. dekoder i komparator – algoritam koji služi za izdvajanje žiga i verifikaciju.

Svaki korisnik ima samo jedan žig koji ga na jedinstven način identificira. Žig se može umetati u bilo koji dokument pomoću algoritma kodiranja, dok se algoritmom dekodiranja on vadi iz označenog dokumenta i jednoznačno se određuje vlasnik i integritet dokumenta. [Digitalni Vodeni žigovi, URL: <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-08-310.pdf> (28.12.2017.)]

Zaštita autorskih prava jedno je od prvih područja za koja je označavanje digitalnim vodenim žigom namijenjeno. Vodeni žig, u ovom slučaju, sadrži informaciju o vlasniku autorskog prava i neprimjetno se ugrađuje u za to namijenjeni sadržaj. Ako korisnici digitalnog sadržaja imaju lagani pristup detektorima vodenog žiga mogu prepoznati i interpretirati ugrađeni vodeni žig te tako identificirati vlasnika autorskog prava.

## 2.1. KAKO DRM FUNKCIONIRA

Otkako se počeo snimati zvuk u 1960-ima, glazba je snimana na gramofonske ploče. Ljudi su tu snimljenu glazbu kupovali u prodavaonicama ploča. Mogli su slušati ploče kod kuće ili na skupovima, a mijenjali su ih s prijateljima. Kopiranje ploča je bio težak i skup poduhvat. Neki ljudi su znali napraviti mix albuma i pjesama koje ne bi bile uključene u finalnu verziju albuma. Također su se na tim mix-ovima našle i snimke izvedbe sa koncerta za koje producerske kompanije nisu imale previše interesa da bi ih objavili.

Pojava kazeta, odnosno magnetskih vrpca (1965.-1966.) kao medija za snimanje donijelo je sa sobom i neke promjene, posebice kada su se prazne kazete stavile na prodaju. Kazete sa originalnim sadržajem bile su kopirane na prazne kazete. Nedugo nakon toga stigao je još veći problem - pojavili su se CD-ovi, a zvuk postao digitalan.

Takozvane pržilice omogućile su ljudima da kopiraju CD-ove i spremaju glazbu na osobna računala. Dodajmo još internet i peer-to-peer<sup>3</sup> (P2P) stranice – producerske kuće i umjetnici su se zaista počeli brinuti. Odjednom je bilo moguće bez problema kopirati i dijeliti glazbu sa gotovo neograničenim brojem korisnika na internetu, što su mnogi iskoristili kako bi besplatno skinuli pjesme, albume, pa čak i cijele diskografije nekog izvođača. Reakcija na pad vrijednosti glazbene industrije bio je Copyright – zaštita autorskog prava – koji je trebalo riješiti problem.

Digitalna revolucija koja je osnažila korisnike da koriste digitalni sadržaj na novi i inovativni način, također je uvelike otežala autorima da kontroliraju distribuciju svoga vlasništva tj. imovine. I ne radi se tu samo o glazbi, već i filmu, video igricama i svim drugim medijskim sadržajima koji mogu biti digitalizirani i dijeljeni uokolo bez problema. DRM je termin koji se koristi za opisivanje bilo koje od tehnika i politika sprečavanja, ili barem smanjenja piratskog pokreta.

Kroz ovaj rad ću dalje spomenuti što je sve DRM, kako vlasnici autorskih prava implementiraju koncepte zaštite, te što nam donosi kontrola digitalnih sadržaja u budućnosti. Ponovno spominjem kako je DRM široki pojam koji se odnosi na bilo koju

---

<sup>3</sup> Koncept umrežavanja računala bez poslužitelja, gdje je svako računalo inteligentna radna stanica, koja pronalazi druga računala putem broadcast ethernet paketa, i komunicira s njima izravno, bez potrebe autorizacije na nekom centralnom poslužitelju.

metodu zaštite i kontrole pristupa zaštićenom materijalu. U suštini, DRM uklanja kontrolu korištenja osobi koja je u posjedu tog sadržaja te ju stavlja u ruke računalnog programa. Metode i aplikacije su beskrajne – evo nekih primjera:

- Kompanija postavlja svoje poslužitelje tako da se blokira prosljeđivanje povjerljive e-pošte.
- Server na kojemu se nalazi e-knjiga ograničava pristup, kopiranje te ispis materijala onako kako ga postavi vlasnik autorskog prava na tu knjigu.
- Filmski studio implementira softver na svoje DVD-e kako bi ograničio broj kopija koje korisnik može napraviti (na dvije kopije).
- Glazbene izdavačke kuće izdaju naslove o vrsti CD-ova koje uključuju komadiće informacija koje imaju zadaću i namjenu da zbune softver s kojim se neovlašteno kopira materijal.

Dok većina potrošača vide DRM kao pretjerano restriktivan, osobito za područje glazbe i filma, ono samo pokušava riješiti problem zaštite prava. Distribucija digitalnog sadržaja na internetu putem mreža za dijeljenje datoteka, učinio je tradicionalni zakon zaštite autorskih prava zastarjelim u praksi. Svaki puta kada netko skine mp3 datoteku koja je zaštićena autorskim pravom, umjesto da kupe original CD, producentska kompanija i umjetnik/izvođač gube novac. Priroda interneta je takva da nije praktično pokušavati tužiti svaku osobu koja prekrši zakon na ovakav način, stoga kompanije pokušavaju povratiti kontrolu nad distribucijom tako da učine stvaranje digitalnih kopija nemogućim.

Problem je kada se kupi DVD, legalno je napraviti vlastitu kopiju za vlastite svrhe i potrebe. To je suština jedne od politika DRM-a koja se naziva Fair use, što obilježava poštenje. Fair use poziva vlasnike originala da ih pošteno koriste (ne krše politike zaštite). No, problem je što mnoge DRM tehnologije ne mogu računati na Fair use metodologiju iz razloga što računalni program ne može donositi subjektivne odluke.

## 2.2. AUTORSKO PRAVO - COPYRIGHT

Copyright u SAD-u izgrađen je po uzoru na razvoj copyright-a u Engleskoj. 1662, zakon o licenciranju nadzire kopiranje davanjem prava na objavljivanje knjiga odabranim tiskarama. Takozvani The Statute of Anne statut, koji je donio Sabor 1710.

godine, utemeljio je autore djela kao vlasnike autorskog prava na period od 14 godina, obnovljiv na novih 14 godina ako je autor i dalje živ nakon isticanja prvog roka. Također, javna domena statuta ograničavala je uvjete autorskog prava te osigurala da nakon kupnje, vlasnik autorskog prava nema više nadzor nad njegovom upotrebom. Ta načela ugrađena su u Ustav SAD-a koji je dao Kongresu moć uspostavljanja uvjeta o autorskim pravima. [The Statute of Anne, 1710. URL: <https://www.copyrighthistory.com/anne.html> (27.03.2018.)]

Autorsko pravo daje ekskluzivno pravo na kopiranje djela koje je zaštićeno. Obuhvaća bilo koji oblik intelektualnog vlasništva, uključujući književna dramska djela, umjetnička i glazbena djela, audio i video zapise, filmove, prijenose poput radija i kabelske televizije, te računalnog softvera. Ukratko, autorsko pravo odnosi se na sva djela koja se mogu naći u fizičkom mediju. Metaforički, DRM štiti bocu koja sadrži intelektualno vlasništvo, ali ne pokriva vino. Stoga, DRM ne štiti u potpunosti ideje, procese sustave, metode, koncepte ili principe, bez obzira na bocu u kojoj će doći. Od kada je prvi put Ustavom autorsko pravo vrijedilo 14 godina od stvaranja, svako toliko se je produžavao taj vijek trajanja istog. Danas, sva autorska prava koja su stvorena nakon 1. siječnja 1978. godine, vrijede za života autora, te još dodatnih 70 godina nakon njegove smrti. Da bi se kvalificirali za autorska prava, djelo mora biti originalno - mora potjecati od autora, a ne biti kopirano iz drugih djela - a količina kreativnosti mora biti više nego trivijalna<sup>4</sup>. [Van Tassel, J. (2016) Digital Rights Management: Protecting and Monetizing Content. Focal Press]

### 2.3. DIGITALNE BRAVE

Digitalne brave potrebne su kako bi se spriječila krađa intelektualnog vlasništva, baš kao što su potrebne fizičke brave kako bi se zaštitila osobna, fizička imovina. Digitalne brave ne postoje samo radi zaštite, već su potrebne za stvaranje nekih mogućnosti koje potrošači žele. Mogu se koristiti u svrhu roditeljske zaštite, kako bi se ograničio pristup sadržaju koji nije primjeren za djecu. Drugi primjer su probni periodi korištenja nekih usluga, prije nego što se osoba odluči za kupnju istih. Digitalne brave se također mogu koristiti kako bi se zaštitila privatnost korporativnih informacija i osobnih informacija kao što su zdravstvene evidencije.

---

<sup>4</sup> Malog značenja. Običan.

Bez restrikcija digitalnog zaključavanja, proizvođači sadržaja ne bi baš imali poticaja dozvoliti ljudima reprodukciju multimedijskog sadržaja na njihovim računalima. DRM također onemogućuje reprodukciju sa legalno kupljenih DVD-a - na računalima s operacijskim sustavom Linux - bez dodatnog softvera. Kupci bi tada morali platiti i dodatni softver, što znači još troškova kako bi koristili ono što su već platili. To bi malo tko prihvatio ravnodušno. [The pros, cons, and future of DRM, URL: <http://www.cbc.ca/news/technology/the-pros-cons-and-future-of-drm-1.785237> (27.02.2018.)]

#### 2.4. OKVIR DRM-a

Idealan DRM sustav je fleksibilan, potpuno transparentan korisniku a ujedno i u potpunosti kompliciran računalnom sustavu (kako ga ne bi probio). Prva generacija DRM softvera zasnivala se je samo na kontroli kopiranja. Druga generacija DRM sustava nastojala je kontrolirati pregled, kopiranje, ispis, izmjenjivanje sadržaja, te gotovo sve što je bilo moguće činiti s digitalnim sadržajem.

DRM sustav djeluje na tri razine:

- Uspostavljanje autorskih prava za komad sadržaja
- Upravljanje distribucijom tog zaštićenog sadržaja
- Kontroliranje što dalje potrošač čini s tim sadržajem nakon distribucije.

Za ostvarivanje ove razine kvalitete upravljanja, potrebno je efektivno definirati i opisati tri entiteta, a to su: korisnik, sadržaj i prava na korištenje, te odnos tj. relacije između njih.

Proizvodi poput onih zaštićenih Macrovision SafeCast-om ili Microsoft Product Activation, koriste web baziranu shemu pružanja dozvole korištenja kako bi se spriječilo ilegalno korištenje sadržaja. Korisnik pokreće instalaciju softvera, nakon čega njegovo računalo automatski kontaktira s license-verification serverom kako bi dobilo dozvolu (pristupni ključ) za instalaciju i pokretanje programa. Ako je korisnikovo računalo prvo koje je zatražilo dozvolu za instaliranje tog određenog softvera, server vraća/šalje ključ. No ako korisnik da taj isti softver prijatelju koji ga proba instalirati, server će odbiti pristup i neće poslati ključ. U ovakvoj shemi korisnik obično mora kontaktirati davatelja tog sadržaja kako bi dobio dozvolu za instaliranje istog na neko

drugo računalo. [Expression Language And Guides The Copyright Holder, URL: <https://www.coursehero.com/file/p4tc8ev/expression-language-and-guides-the-copyright-holder-through-the-process-of/> (27.02.2018.) ]

Nešto manje u korištenju je metoda digitalnog vodenog žiga. FCC<sup>5</sup> zahtjeva na tzv. Broadcast flag koji daje na znanje digitalnom video snimaču smije li određeni program snimiti ili ne. Broadcast flag dio je koda koji se šalje uz digitalni signal. Ako taj kod kaže da je sadržaj zaštićen, DVR i DVD snimači ne mogu snimiti taj sadržaj programa. Ovakav DRM jedan je od zahtjevnijih jer zahtjeva također i opremu i medije koji mogu pročitati taj Broadcasting flag. Philipsov VCPS (Video Content Protection System) format čita Broadcasting flag i odeduje može li ili ne uređaj snimiti program. Disk sa nezaštićenim sadržajem se može pokrenuti na svim DVD čitačima dok se oni sa Broadcasting flag kodom mogu pokrenuti samo na onim čitačima koji sadržavaju VCPS.

Hellman Production nudi zanimljiv pristup zaštiti DVD proizvoda sa RipGuard-om. Ne fokusiraju se na disk već na DVD pržilice. RipGuard iskorištava propuste softvera za kopiranje diskova te na taj način sprječava kopiranje. RipGuard je kod koji se stavlja skupa sa softverom na DVD, a njegova svrha je da zbuni kod poznat pod nazivom DeCSS – mali program koji omogućuje čitanje i kopiranje šifriranih DVD-a. RipGuard aktivira propuste programa za kopiranje DVD-a, te gasi proces kopiranja. Oni fanatični korisnici DVD-a su našli način da zaobiđu i RipGuard nekorištenjem softvera koji se služe DeCSS-om ili podešavanjem i poboljšavanjem DeCSS koda. DMCA<sup>6</sup> je je 1998. godine učinio ilegalnim gašenje i onеспособljavanje DRM sustava. Unatoč tome mnogi i dalje aktivno traže i objavljuju načine zaobilaženja DRM ograničenja. [RipGuard copy protection - process, URL: <http://www.hellmanproduction.com/cd/dvd-replication/ripguard-copy-protection-process.html> (10.03.2018.) ]

---

<sup>5</sup> Federal Communications Commission je nezavisna agencija vlade SAD-a koja regulira međudržavne komunikacije putem radija, televizije, žica, satelita i kabela u svih 50 država (SAD-a), nekim predjelima Kolumbije te ostalim američkim teritorijima.

<sup>6</sup> DMCA je zakon o elektroničkim autorskim pravima, potekao u SAD-u, te sprovodi dva sporazuma iz 1996. godine koje je navela Svjetska organizacija za intelektualno vlasništvo (skraćeno engl. WIPO). Navodi kako je kriminal proizvodnja i širenje tehnologije, uređaja ili usluga namijenjenih zaobilaženju mjera koje kontroliraju pristup djelima zaštićenim autorskim pravom. Drugo, čin zaobilaženja kontrole pristupa, bez obzira da li postoji stvarna povreda autorskog prava - također je kažnjivo djelo.

## 2.5. RIGHTS EXPRESSION LANGUAGE

Dva jezika za izražavanja prava u digitalnome obliku koji se u današnje doba koriste su: MPEG Right Expression Language (MPEG REL) te Open Digital Rights Language (ODRL). Oba su XML<sup>7</sup> bazirana jezika. ODRL koristi terminologiju poput: izvod (engl. Excerpt), instalirati (engl. Install), posuditi (engl. Lend), izmjeniti (engl. Modify), reproducirati (engl. Play), prodati (engl. Sell). Također postavlja i ograničenja: fiksni iznos (engl. fixed amount), interval (engl. interval), raspon (engl. Range), te definira način plaćanja (engl. feeType): plaćanje unaprijed (engl. Prepay), te naknadno plaćanje (engl. Postpay). [How Digital Rights Management Works, URL: <https://computer.howstuffworks.com/drm2.htm> (27.02.2018.)]

RightExpress softver koristi MPEG REL<sup>8</sup> jezik i vodi nositelja prava kroz čitav proces: definiranje sadržaja, definiranje korisnika, te definiranje prava korištenja. Moguće je postaviti i razine pristupa, te metode šifriranja sadržaja, stvaranje prilagođenog sučelja koje korisnicima omogućuje dobivanje sadržaja baziranog na temelju tih postavki., te razvijanje modela koji potvrđuje identifikaciju korisnika te prati korištenje sadržaja.

## 2.6. PRIMJER PRIMJENE DRM-A

Uzmimo za primjer DRM sustav koji kontrolira stranicu za skidanje MP3 sadržaja. Jana Janić se ulogira na stranicu na kojoj je pretplaćena kako bi mogla skinuti pjesmu Amsterdam od Luke Nižetića. Njezina pretplata daje joj na pravo skinut pet pjesama mjesečno. Tu imamo dva entiteta, a to su Jana Janić te sadržaj (pjesma Amsterdam). Jana vjerojatno ima svoj jedinstveni ID putem kojeg ju se identificira, a svaka pjesma svoj Product ID ili sl. Ono što je kompliciranije je identificiranje prava, odnosno načine na koje Jana može i ne može koristiti taj sadržaj. Može li ga skinuti ili je već potrošila broj pjesama koje može skinuti na mjesec? Smije li kopirati sadržaj i da li skida šifrirani sadržaj sa odgovarajućim ključem? Smije li uzeti uzorak iz te pjesme i koristiti ga u skladbi nekog vlastitog sadržaja ili je datoteka zaključana? Prava korištenja ne uključuju samo dozvole i ograničenja, već i sve obveze vezane uz transakciju, na primjer: da li Jana mora dodatno platiti za skinuti tu datoteku? To bi bilo uključeno u relaciju između

---

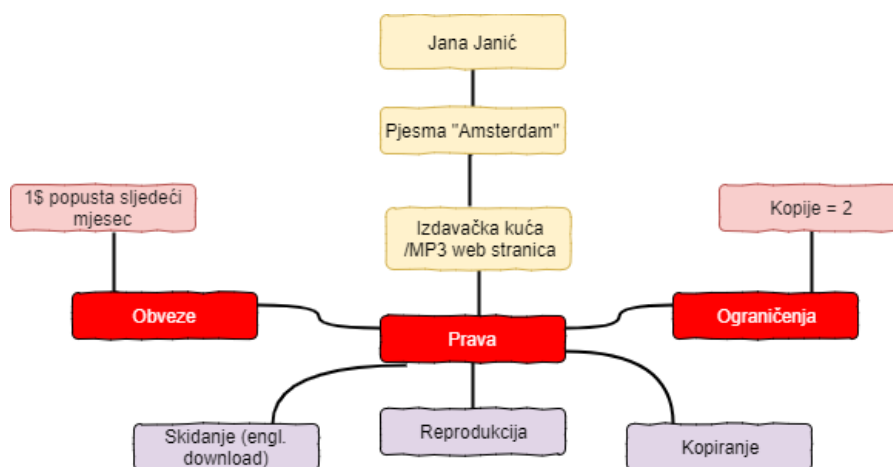
<sup>7</sup> XML je kratica za EXtensible Markup Language - odnosno jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. Princip realizacije je vrlo jednostavan: odgovarajući sadržaj treba se uokviriti odgovarajućim oznakama koje ga opisuju i imaju poznato, ili lako shvatljivo značenje.

<sup>8</sup> Hrv. Jezik izražavanja prava. Strojni jezik koji deklarira prava i dopuštenja.



Jane , pjesme i prava. [How Digital Rights Management Works, URL: <https://computer.howstuffworks.com/drm3.htm> (26.02.2016.) ]

Recimo da je, Jana Janić skinula tek tri pjesme ovaj mjesec, tako da pjesma „Amsterdam“ ulazi u prava njezine pretplate. I recimo da će dobiti još dodatno 1\$ popusta na pretplatu za sljedeći mjesec ako skine ovu pjesmu. Jana bi trebala moći kopirati tu pjesmu pod Fair use uvjetom, no možda je ograničena na samo dvije kopije, a nositelj autorskog prava uskraćuje pravo na korištenje tog sadržaja u neke vlastite svrhe. Struktura toga procesa skidanja pjesme prikazana je na slici 3.



Slika 3 Struktura i procedure skidanja pjesme zaštićene DRM tehnologijom

Izvor: <https://computer.howstuffworks.com/drm3.htm>

Imajmo na umu kako status korisnika uvijek ostaje isti svaki put kada se ulogira, no relacija između korisnika, sadržaja i prava se može promijeniti. DRM shema mora biti prilagodljiva promjenama. Tako da kada bi Jana nadogradila svoju pretplatu na bezgraničan broj skidanja pjesama umjesto samo pet mjesečno, DRM softver se mora prilagoditi tom novom odnosu. Shema mora biti povezana s web stranicom kako bi se odnos podesio u trenutku. Ovo je jedan od razloga zašto je teško postaviti DRM da funkcionira savršeno i bez grešaka. [How Digital Rights Management Works, URL: <https://computer.howstuffworks.com/drm3.htm> (26.02.2016.) ]

Prilično je jednostavno dopustiti Jani da kopira pjesmu samo dva puta. Računalo razumije „dva“ (puta), no ono što računalo ne razumije je da nakon što je Jana kopirala pjesmu na mp3 player i na laptop, kupila je novo računalo i treba ponovo kopirati tu datoteku na novo računalo, koje je njeno.



Slika 4 Zabranjena kopiranja zbog DRM ograničenja broja kopija

Izvor: <https://computer.howstuffworks.com/drm4.htm>

Fair use<sup>9</sup> nije uvijek moguće lako i jednostavno odrediti i definirati. Stoga su mnoge kompanije pokušale isključiti bilo kakvo pravo potrošača, odnosno vlasnika digitalnog sadržaja da radi s istim što god želi. Naj aktualnije DRM sheme po mnogima prelaze granicu od zaštite neovlaštenog kopiranja do prestroge kontrole nad digitalnim sadržajem.

Česta DRM shema šifriranja pruža ključ za šifriranje koji radi zauvijek. U tome slučaju ključ mora biti povezan sa ID brojem korisničkog računala. Tako, ključ će dešifrirati sadržaj samo kada mu se pristupa sa računala na kojemu je softver prvenstveno instaliran. U protivnome, vlasnik bi mogao proslijediti ključ drugima zajedno sa zaštićenim softverom i on bi funkcionirao.

---

<sup>9</sup> Fair use je doktrina u Zakonu SAD-a koja dopušta ograničenu upotrebu materijala zaštićenih autorskim pravom, bez potrebe da prvo dobije dozvolu vlasnika autorskog prava. Također jedno je od ograničenja koja bi trebala uravnotežiti interese vlasnika autorskih prava s javnim interesom za širu distribuciju i upotrebu kreativnih djela, no u slučaju kršenja tog ograničenja, postupak kopiranja smatra se kriminalnim, te kažnjivim.

### 3. ULOGA DRM TEHNOLOGIJA NA TRŽIŠTU DIGITALNIH SADRŽAJA

Temeljna namjena DRM-a jest ograničenje pristupa zaštićenim sadržajima, odnosno upravljanje pristupom sukladno ovlaštenjima koje je korisnik dobio od nositelja prava. Osim toga, DRM tehnologija nalazi svoje mjesto i na području ustroja hardverskih i softverskih platformi koje služe distribuciji zaštićenih sadržaja.

Nositelji prava (uglavnom velike multinacionalne korporacije sa snažnim utjecajem u medijskoj industriji) u pogledu digitalne distribucije zaštićenih sadržaja najčešće biraju jednu od dvije pozicije ili sami organiziraju digitalne distribucijske kanale kao nositelji prava i distributeri (poput japanskog Sonyja, primjerice u pogledu konzole Playstation distribucije igara namijenjenih toj platformi ili američkog Amazona u pogledu distribucije elektroničkih knjiga na vlastiti uređaj Kindle) ili to čine u suradnji s nekim drugim poduzetnicima (tako surađuju npr. brojni američki glazbeni i filmski studiji kao nositelji prava i Apple kao distributer zaštićenih sadržaja koje nudi preko iTunes servisa).

Sustavi ograničenja pristupa sadržajima temeljeni na DRM tehnologiji mogu znatno ograničiti korisnika u pogledu korištenja tako pribavljenog sadržaja s raznim drugim uređajima i servisima koje on rabi. Istovremeno, sam DRM softver ili hardver također čini proizvod, odnosno novo tržište gdje nositelje prava na zaštićenom sadržaju zanima odabir kvalitetnih i efikasnih tehnoloških metoda zaštite po konkurentnoj cijeni.

Preko utjecaja DRM-a na distribucijske sustave utječe se i na sekundarna tržišta, što može indirektno utjecati na primarna tržišta. Kada se razmatra tržišni utjecaj DRM tehnologija, za početak treba definirati tržišta na kojemu se on istražuje. Na primjeru jedne od najstarijih usluga za digitalnu distribuciju sadržaja internetom, Appleova sustava iTunes, dokazano je da takvo određenje nije nimalo jednostavno. [Dragičević D., Katulić, T. (2013.) Utjecaj DRM tehnologija na tržište digitalnih sadržaja]

#### 3.1. TRŽIŠNE POSLJEDICE UPOTREBE DRM TEHNOLOGIJA

Osim osnovne zadaće ovih tehnologija, koja je zaštita digitalnog sadržaja od neovlaštene distribucije i korištenja, te ograničavanja razina korisničkog pristupa sadržaju. Još jedna važna zadaća DRM-a, a to je mogućnost diversifikacije samog pristupa sadržaju različitim naplatnim modelima – omogućavanje segmentacije tržišta –

koja je u ovisnosti sa korisničkom platnom sposobnosti<sup>10</sup> (naknadi koju je spreman platiti za određeni sadržaj). Nositelji prava digitalnog sadržaja, ovisno o okolnostima na pojedinom tržištu mogu prilagoditi cijene svojih proizvoda.

Drugačiji model segmentacije tržišta predstavlja upotreba specifičnih, vlasničkih, međusobno nekompatibilnih DRM standarda. U digitalnom okruženju distribucija sadržaja korisnike upućuje na distribucijske servise poput Apple-ovog iTunes sustava, Microsoftovog Windows Marketplacea ili Google Marketa odnosno GooglePlay usluge. Ako su ti sadržaji zaštićeni nekom DRM tehnologijom, postoji velika vjerojatnost da će korisnik plaćanjem i preuzimanjem tog sadržaja licencirati isti za upotrebu samo na uređajima kompatibilnima s tim servisom. Ako korisnik pribavi i plati sadržaj putem iTunesa, isti neće raditi u Windows Media Playeru ili na nekoj od Google-ovih platformi. Ova ograničenja imaju značajan utjecaj na iznimno važnu korisnikovu percepciju vrijednosti digitalne kopije, jer ona više ne nudi mogućnost korištenja koje je korisnik mogao očekivati od sadržaja distribuiranog na fizičkom podatkovnom mediju. [Dragičević D., Katulić, T. (2013.) Utjecaj DRM tehnologija na tržište digitalnih sadržaja]

Moj vlastiti primjer, gdje sam se suočio s DRM -om tiče se glazbene industrije i GooglePlay usluge. Kupio sam glazbeni album putem Google Music trgovine, uredno ga platio, nakon čega je album skinut na moj uređaj. Tako je barem bilo prikazano. No, nije moguće ikako doći do tih datoteka, osim putem aplikacije Google Glazba. Samo ta aplikacija može reproducirati te pjesme. A ja kao korisnik, ne mogu ih prebaciti na niti jedan drugi uređaj, te mogu koristiti i slušati taj album samo putem te aplikacije, te uz prijavu s mojim računom, putem kojega sam izvršio kupnju.

### 3.2. DRM KAO RIZIK ZA TRŽIŠNO NATJECANJE

Postalo je jasno da DRM, kako je upotrijebljen u Apple-ovu slučaju, ima snažan anti-tržišni odnosno anti-konkurencijski potencijal. U širem smislu, mogućnost da se DRM tehnologija upotrijebi u takvu svrhu više nije sporna. Apple-ov slučaj pokazuje da je najveća opasnost za povredu pravila tržišnog natjecanja mogućnost da se DRM

---

<sup>10</sup> Očekivanje da će zapadnoeuropski korisnik ili stanovnik SAD-a plaćati istu cijenu za glazbeni CD, DCD s filmskim naslovom ili softversku licenciju kao i stanovnik Kine ili Indije u najmanju ruku je nerealno. Tako npr. softverske kompanije poput Microsofta već desetljećima znatno povoljnije prodaju posebne inačice svog softvera namijenjene tržištu zemalja u razvoju, iako se taj softver bitno funkcionalno ne razlikuje od onog koji se prodaje na tržištima Europe ili SAD-a.

tehnologija upotrebljava unutar informacijskog sustava čije su komponente zaštićene pravima intelektualnog vlasništva (patentima, autorskim pravom ili neobjavljenim programerskim tehnikama zaštićenima institutom poslovne tajne).

Očigledno je kako je Apple podigao zidove oko svojih uređaja i softvera. Pojavio se je pojam Apple Ecosystem. Apple radi mnogo uređaja (Homepad, iPhone, iPad, Mac, Apple Watch, Apple TV) no i programe i aplikacije koje ih sve povezuju (AirPlay, AirDrop, Continuity, iCloud, itd.). Na taj način privlače, a možda i suptilno tjeraju korisnike da kupuju samo njihove uređaje, te uz njih i programe i aplikacije koje dolaze s njima. Recimo da posjedujemo iPhone i iPad, te poželimo kupiti i neki SmartWatch. Na tržištu postoji mnogo proizvođača i izbora, no zašto sad kupiti Samsung-ov SmartWatch – koji nije kompatibilan sa Apple uređajima koje posjedujem - iako je možda kvalitetniji ili nudi neku bolju opciju. Naravno da ćemo odabrati Apple Watch, jer on će se uklopiti u taj Ecosystem.

Dok se na tržištu natječe nekoliko DRM tehnologija, Europska Komisija neće smatrati da postoji problem oko tržišnog natjecanja – stav je koji imaju neki od teoretičara poput Mazziottija u pogledu kriterija za procjenu utjecaja DRM-a na tržište. No, ne uzima u obzir specifičnosti i brz razvoj tržišta digitalnih sadržaja, kao ni brzinu evolucije povezanih hardverskih i softverskih platformi. [Mazziotti, G. (2007.) EU Digital Copyright Law and the End-User]

## 4. IMPLEMENTACIJA DRM-A U RAZLIČITIM VRSTAMA AUTORSKIH DJELA

Autorska prava pojavljuju se u raznim oblicima autorskih djela. Svaki intelekt je za sebe poseban te se može manifestirati kroz sofisticirane kanale. Ako netko napiše knjigu – te ju digitalizira – implementirati će neku od DRM opcija koje se koriste za zaštitu e-knjiga. Dok će glazbena grupa, odnosno njihova producentska kuća zaštititi njihova autorska prava nekom od DRM opcija za zaštitu glazbe. Pored ova dva primjera DRM se još implementira u drugim vrstama autorskih djela poput filma, dokumenata, računalnih igara, online servisa za strujanje, te raznih drugih multimedijalnih sadržaja.

Ovo poglavlje poslužiti će za predstavljanje vrsta i načina zaštite u različitim oblicima autorskih djela. Također predstaviti primjere, te neke probleme i kontroverze.

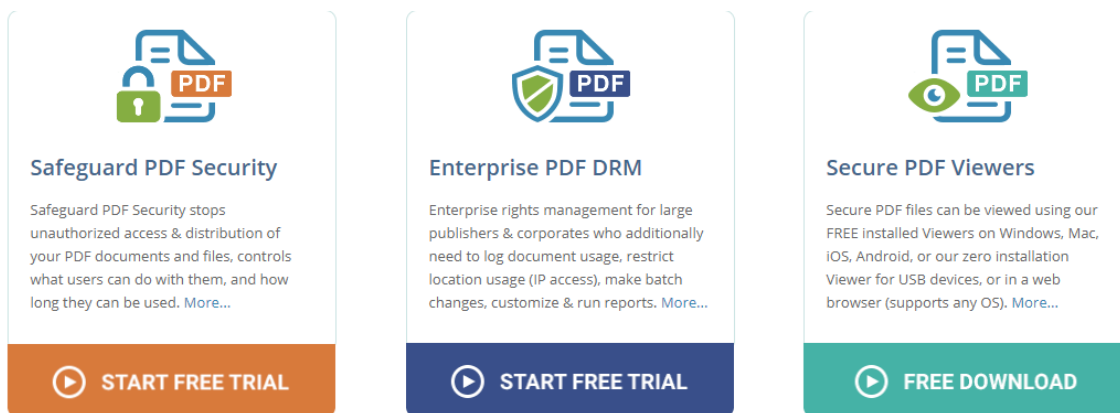
### 4.1. DOKUMENTI

Zaštititi dokumente moguće je na razne načine također. Postoji razni softveri i pružatelji te usluge, ja ću navesti i prikazati dva primjera: Locklizard, te Drumlin.

Oba pružaju mnoštvo opcija kako zaštititi dokument, a Locklizard nudi:

- sprečavanje dijeljenja dokumenta, rok trajanja dokumenta (nakon čega ih se više ne može koristiti),
- sprečavanje mogućnosti ispisa dokumenta,
- sprečavanje kopiranja, uređivanja te pohrane dokumenta, onemogućavanje snimke zaslona dok je dokument otvoren, povlačenje dokumenta iz uporabe (primjer kako je Amazon povukao kopiju Orwell-ove knjige),
- zaključavanje dokumenta na uređajima, određenim domenama i IP adresama (npr. regionalno zaključavanje putem IP-a, ili specifično zaključavanje gdje je dokument dostupan samo na uređajima koji koriste IP s područja tvrtke u kojoj se koriste),
- nadziranje dokumenta (broj pregleda, ispisa i od strane kojeg korisnika, itd.),
- stvaranja vodenog žiga na dokumentu,
- daljinsko brisanje dokumenata,
- te uslugu pohrane dokumenata na njihovim serverima, te distribuciju.

Na slici 5, sa službene stranice Locklizard-a - ponuda dviju opcija od kojih se jedna fokusira na pojedince, a druga na tvrtke. Uz to potreban je i njihov preglednik, kako bi se ti zaštićeni dokumenti mogli otvoriti.

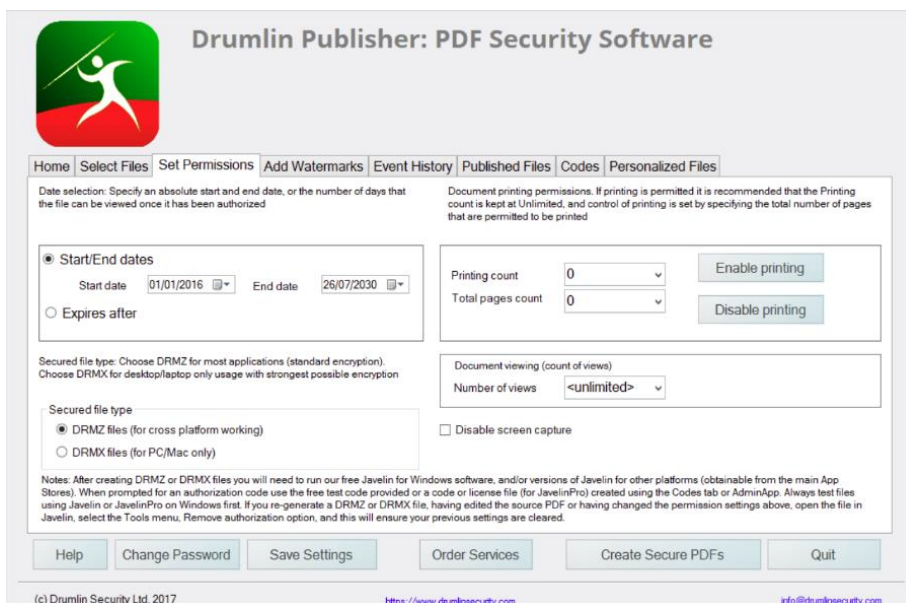


Slika 5 Opcije koje nudi Locklizard za zaštitu dokumenata

Izvor: [https://www.locklizard.com/digital\\_rights\\_management\\_products/](https://www.locklizard.com/digital_rights_management_products/)

Otprilike, prva opcija je da svaki korisnik može birati vrstu zaštite pojedinačno za svaki dokument, dok u ovoj opciji prilagođenoj tvrtki, ona određuje skupno uvjete zaštite za sve dokumente na njenom području, te se koristi i prije navedena zaštita na području tvrtke putem IP adrese. Ne mogu svi korisnici mijenjati te uvijete i politiku zaštite, već samo oni s administrativnim činom.

Drumlin je baziran na istom principu, stoga ću samo prikazati kako izgleda sučelje Drumlina, te da se vide neke od opcija koje nudi (Slika 6).



Slika 6 Drumlin sučelje

Izvor: <https://www.drumlinsecurity.com/>

## 4.2. FILM

Za upravljanje digitalnim pravima pri rukovanju video sadržajima najčešće se koriste CSS sustav (sada već zastarjeli), noviji PMP sustav (integriran u Vista operacijskim sustavima), te AACS standard.

Kratica CSS stoji za Content Scrambling System. Ono je jedno od nekoliko metoda zaštite koje se danas koriste kako bi se zaštitilo neovlašteno kopiranje, distribucija, te reprodukcija putem drugih uređaja koji nisu DVD diskovi. CSS metodu su razvili članovi DVDCAA (DVD Copy Control Association), koje uključuju kompanije tzv. *U.S. motion picture industry* (kompanije koje se bave produkcijom filmskih sadržaja) te *consumer electronics industry* (kompanije koje se bave proizvodnjom uređaja koji omogućuju reprodukciju tih sadržaja). Najviše zasluga za stvaranje CSS-a pripada kompanijama Matsushita i Toshiba, koje su prve uložile veći napor za razvijanje metoda šifriranja i dešifriranje DVD filmova.

AACS (engl. Advanced Access Content System) je jedna od tehnologija upravljanja digitalnim pravima. Riječ je o standardu za distribuciju digitalnih sadržaja i upravljanje pravima njihova korištenja namijenjenom ograničenju pristupa i onemogućavanju neovlaštenog umnožavanja sadržaja pohranjenog na optičkim diskovima nove generacije (HD DVD i Blu-ray diskovi). AACS je izradio AACS LA konzorcij kojeg čine poznate svjetske tvrtke kao što su Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM, Toshiba i Sony.

Zajedno sa sadržajem zapisuju se podaci o uređajima i aplikacijama kojima nije dozvoljen pristup sadržaju te jedinstveni podaci za svaki pojedini medij. Uz to, uređaji i aplikacije za reprodukciju takvog sadržaja dobivaju vlastite ključeve pomoću kojih, ukoliko se ne nalaze na popisu onih koje za to nemaju ovlasti, mogu dešifrirati zaštićen sadržaj i reproducirati ga na korisničkom uređaju. AACS posjeduje mogućnost povlačenja kompromitiranih ključeva iz uporabe te implementacije novih u novijim inačicama zaštićenih sadržaja.

AACS sustav za zaštitu digitalnog sadržaja kao i sve ostale tehnologije upravljanja digitalnim pravima od samih početaka razvoja prate dva velika nedostatka. Prvi je vezan uz ograničavanje uporabe sadržaja vlasnicima legitimnih kopija čime im se otežava njihovo korištenje. S druge strane, postavlja se pitanje isplativosti ulaganja velikih novčanih sredstava i ljudskih resursa u tehnologiju koja je u današnjim uvjetima



osuđena na neuspjeh. Razlog je jednostavan, vlasnici legitimnih kopija zaštićenog sadržaja moraju biti u mogućnosti takav sadržaj koristiti i to na način da im je omogućen pristup svim alatima i informacijama potrebnim za njegovu reprodukciju. Ipak, nakon predaje kriptografskog algoritma, zajedno s ključevima i šifriranim sadržajem korisnicima na današnjim osobnim računalima, samo je pitanje vremena kada će doći do kompromitiranja sustava. [AACS – Sustav za zaštitu digitalnog sadržaja, URL: <https://www.cis.hr/files/dokumenti/CIS-DOC-2011-02-003.pdf> (10.03.2018.) ]

#### **USPOREDBA AACS-A i CSS-A**

Sigurnost AACS sustava stalan je predmet rasprava među stručnjacima iz različitih područja. Kao nasljednik sustava za zaštitu sadržaja na DVD-ima (CSS), AACS je kvalitetu zaštite trebao unaprijediti ispravljajući najznačajnije mane prethodnika. Problem je u tome što je CSS nakon 1999. godine i objave programa DeCSS (koji može dešifrirati bilo koji sadržaj zaštićen CSS sustavom) u potpunosti izgubio funkcionalnost.

Osnovna razlika između AACS-a i CSS-a leži u organizaciji ključeva dešifriranja unutar uređaja za reprodukciju. Kod CSS-a svi uređaji istog modela imaju jednak ključ za dešifriranje. Sadržaji su šifrirani prema ključu ovisno o naslovu, a taj je ključ zatim šifriran pomoću ključa vezanog uz model uređaja. Zbog toga svaki disk sadrži nekoliko stotina ključeva šifriranja, po jedan za svaki licencirani model uređaja za reprodukciju. Takav pristup omogućuje opoziv tek određenog modela uređaja za reprodukciju izuzimanjem njegovog ključa dešifriranja iz budućih izdanja. Dodatni nedostatak je i povećana ranjivost zbog jednog ključa pohranjenog u velikom broju uređaja, što jasno pokazuju brojni slučajevi probijanja zaštite iz sredine 90-ih godina prošlog stoljeća.

Kod AACS-a svaki uređaj ima jedinstven skup ključeva za dešifriranje koji se koriste u mehanizmu difuznog šifriranja (ključevi uređaja). Takav pristup vlasniku licence omogućuje opozivanje pojedinog uređaja za reprodukciju, odnosno njegova skupa ključeva za dešifriranje. Ako zlonamjerna korisnik probije zaštitu određenog uređaja i objavi njegove ključeve, AACS LA<sup>11</sup> može povući kompromitirane ključeve uređaja i onemogućiti reprodukciju budućih naslova na spomenutom uređaju. [What is AACS, URL: <https://www.aacsla.com/what/overview> (11.03.2018.)]

---

<sup>11</sup> Upravlja sadržajem pohranjenim na optičkim medijima, za potrošačku upotrebu na osobnim računalima te uređajima.

## MARLIN

Ovaj sustav zaštite je razvijen i održavan od otvorene grupacije koja je poznata pod nazivom Marlin Developer Community (MDC) i licencirana od strane Marlin Trust management Organisation (MTMO). Osnovana je 2005. godine udruživanjem pet kompanija: Intertrust, Panasonic, Philips, Samsung i Sony. Marlin DRM se koristi širom svijeta. U Europi ga koriste HDForum (Francuska), Tivu (Italija), YouView (UK). U Japanu acTVila IPTV koristi Marlin šifriranje video strujanja.

Sve su to sudionici Open IPTV Forum konzorcija – standardizirane organizacije koja je fokusirana na definiranje i objavljivanje standarda i protokola za end-to-end Internet Protocol televizijske usluge (IPTV).

Na primjer u Italiji je Tivu<sup>12</sup> taj koji daje i emitira televizijske kanale putem interneta svojim korisnicima. Nude razne programe i pretplate, ovisno o paketu koji korisnik plati, dobije prava, te također i ograničenja za korištenje njihove usluge. [Programmi, film e serie tv on demand, URL: <http://www.tivuon.tv/cosa-e-tivuon.aspx> (11.03.2018.)]

### 4.3. E-KNJIGE

Elektroničke verzije knjiga; e-knjige, koje se čitaju na osobnim računalima, e-book čitačima ili putem aplikacija za čitanje tih knjiga, obično koriste neku DRM tehnologiju kako bi limitirali kopiranje, ispis i dijeljenje istih. Najčešće ograničenje je limitiran broj uređaja na kojima se može čitati, te nemogućnost ispisa i ikakvog dijeljenja i daljnje distribucije. No govorim najčešće, jer postoje i neki e-izdavači (engl. e-publisher) koji dozvoljavaju ispis i kopiranje.

Od kolovoza 2012. godine, postoji pet glavnih (vodećih) formata e-knjiga, koji su: EPUB, KF8, Mobipocket, PDF, i Topaz. Amazon Kindle koristi KF8, Mobipocket i Topaz, no također podržava i izvorne PDF formate e-knjiga i ostalih PDF datoteka. Drugi čitači e-knjiga uglavnom koriste e-knjige EPUB formata no s različitim DRM shemama.

Četiri glavne DRM sheme koje se danas koriste su po jedna od Adobe-a, Amazon-a, Apple-a, te Marlin Trust Management Organization (MTMO). Adobe ADEPT DRM primjenjuje se na EPUB I PDF datoteke, te se mogu čitati i na nekoliko drugih "third

---

<sup>12</sup> Tivultalia S.p.A. (Societa per azioni), kontroliraju sva prava njihove (talijanske) mreže na televizijske kanale.

party" čitačima, jednako kao i putem Adobe Digital Editions (ADE) softvera. Barnes & Noble koristi DRM tehnologiju koju pruža ADOBE, primjenjivu na EPUB te starijih PDB (Palm OS) formatima e-knjiga. U listopadu 2014 Adobe je objavio verziju 4.0.1 softvera koji šalje podatke Adobeu u sigurnosnom prijenosu koristeći HTTPS. Amazon je prilagodio originalno Mobipocket šifriranje te ju primjenio na Amazon .awz4, KF8 te Mobipocket formate e-knjiga. Topaz formati e-knjiga imaju svoj sustav šifriranja. Apple FairPlay DRM se primjenjuje na EPUB, a trenutno ih može čitati samo Apple iBooks aplikacija na iOS uređajima i MacOS računalima. Marlin DRM razvijenje i održavan u otvorenoj industrijskoj grupaciji poznatoj pod nazivom Marlin Developer Community (MDC) i licencirana je od strane MTMO-a. Marlin je osnovala grupa od pet tvrtki: Intertrust, Panasonic, Philips, Samsung i Sony. Kno online izdavač knjiga koristi Marlin kako bi zaštitio e-knjige koje se prodaju u EPUB formatu. Ove knjige mogu se čitati samo na aplikaciji Kno za iOS i Android.

Jedan primjer gdje je DRM uzročnik skandala između korisnika i Amazona dogodio se u srpnju 2009. godine. Amazon je korisnicima Amazon Kindlesa obrisao sve kupljene kopije George Orwellovih e-knjiga *Animal Farm* (1945) te *Nineteen Eighty-Four* (1949), no vratio im je sredstva za kupljene knjige.

Komentatori su ovaj događaj prozvali *orvelijanskim*<sup>13</sup> što je ironično, te usporedili Amazon s Big Brotherom iz Orwellove knjige "Nineteen Eighty-Four". Nakon što je Amazonov CEO Jeff Bezos uputio javnu ispriku svima, Free Software Foundation je objavio članak u kojemu piše kako je to samo još jedan primjer prevelike moći Amazona - kada [daljinski] mogu cenzurirati ono što ljudi pročitaju kroz svoj softver - te su pozvali Amazon da učini čitač e-knjiga slobodnim za uporabu te izbace DRM. Naknadno, Amazon je objavio razlog zbog kojega su obrisali te određene e-knjige, rekavši da su one bile neovlaštene reprodukcije Orwellovih djela koja nisu bila u javnoj domeni te tvrtka koja ih je prodavala na Amazonu, nije imala prava na njih. [Amazon Erases Orwell Books From Kindle Devices. New York Times URL: <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>

(11.03.2018.)]

---

<sup>13</sup> engl. Orwellian - pridjev - opisuje situaciju, ideju ili društveno stanje koje George Orwell identificira kao destruktivno za blagostanje u slobodnom i otvorenom društvu. Označava stav i brutalnu politiku drakonskih kontrola propagandom, nadzorom, dezinformiranjem, poricanjem istine, ...

Web stranice poput library.nu (ugašena po sudskom nalogu 15.veljače 2012.), BookFi, BookFinder, Library Genesis, te Science Hub omogućuju preuzimanje e-knjiga kršenjem autorskih prava.

#### 4.4. RAČUNALNE IGRE

##### **OGRANIČAVANJE AKTIVACIJA INSTALACIJE**

Autori računalnih igara koriste DRM kako bi ograničile broj sustava na kojima se može instalirati igra, zahtijevajući provjeru autentičnosti s on-line poslužiteljem. Većina igara s tim ograničenjem dopuštaju tri ili pet instalacija, iako neke dopuštaju oporavak broja instalacija nakon što se igra deinstalira. To ne samo da ograničava korisnike koji imaju više od ograničenog broja računala u svojim domovima, već može biti i problem kod neočekivanog obnavljanja ili nadogradnje operativnog sustava, te formatiranja tvrdog diska. Ovisno o tome kako se implementira DRM, ovi slučajevi se mogu računati kao nova instalacija igre, čime ona potencijalno može postati neupotrebljiva nakon određenog razdoblja, čak i ako se koristi za samo jedno računalo.

Sredinom 2008. godine, objavljivanjem igre Mass Effect, započeo je val igara koje se primarno koriste SecuRom14 tehnologijom, te zahtijevaju autentifikaciju s serverom. Igra Spore dovela je do protesta zbog ograničavanja kopija na samo tri, što je dovelo do toga da je postala najpiratiziranija igra u 2008. Godini. Na stranici TorrentFreak, Spore je predvodila listu top 10 torrenta. [Top 10 Most Pirated Games of 2008, URL: <https://torrentfreak.com/top-10-most-pirated-games-of-2008-081204> (10.03.2018.) ]

Ali naravno to nije bio ekskluzivni razlog za piratizaciju. I druge igre poput Assassin's Creed, COD 4, Crysis, itd. bile su "krekirane" iako je njihov SafeDisc DRM dozvoljavao neograničen broj instalacija, te nije zahtijevao on-line aktivaciju.

##### **KONSTANTNA ONLINE PROVJERA AUTENTIČNOSTI**

Mnogi izdavači zadržali su se na online DRM-u od kraja 2008. te početkom 2009. godine nadalje, uključujući Electronic Arts, Ubisoft, Valve, te Atari. Koristi se tzv. Always-On DRM shema, koja zahtjeva od korisnika da konstantno bude spojen na server putem interneta kako bi koristio proizvod. Najveći nedostatak ove tehnologije je da svaki put kada server za provjeru autentičnosti "padne" ili neko područje ostane bez

---

<sup>14</sup> SecuRom softver ograničava broj istodobno aktiviranih računala putem istog ključa, te ključ nije deinstaliran nakon uklanjanja igre.

pristupačnosti internetu, apsolutno sprječava ljude da igraju igru. Također veliki je nedostatak da ako se ikada ugase ili zatvore serveri, igra postaje potpuno beskorisna i ne igriva.



Slika 7 Prekid komunikacije s poslužiteljem

Izvor: <http://www.jokergameth.com/board/showthread.php?t=195893>

Računalna igra „Need for Speed (2015.)“, namijenjena je u potpunosti igranju samo putem servera. Kako multiplayer (engleski izraz za mogućnost igranja više igrača u istome trenutku) tako i single player (engleski izraz za mogućnost igranja samo jednim igračem u istome trenutku). Electronic Arts su izjavili kako je to zbog toga što je igra stalno bila nadograđivana, te se je svijet u igri konstantno širio putem stalnih nadogradnji. Također zagovarali su da se fotke iz igre objavljuju na Autologu, kako bi igrači mogli skupiti više bodova njihovim objavljivanjem ako one postanu relevantne. To je sve dovelo samo do sve više kritika, te je taj nastavak igre postao sve manje popularan, a općenito Need for Speed manje igran na svim platformama. Zahvaljujući ovome konfliktu, EA je odlučio da sljedeći nastavci ipak budu igrici i u izvan mrežnom modu (engl. offline mode), te je i posljednji nastavak igre „*Need for Speed: Payback*“ stigao na tržište sa izvan mrežnom single player modom. [Ubisoft undone by anti-DRM DDoS storm. URL:

[https://www.theregister.co.uk/2010/03/08/ubisoft\\_anti\\_drm\\_hack\\_attack](https://www.theregister.co.uk/2010/03/08/ubisoft_anti_drm_hack_attack) (27.02.2018.) ]

## PETLJANJE PO SOFTVERU

Vjerojatno najzabavnija DRM shema koju je iskoristila Bohemia Interactive, petljanje je po softveru (engl. Software Tampering). Prvi put uvedeno na igri "Operation Flashpoint: Cold War Crisis", u kojoj - ukoliko se s pravom posumnja da je igra u neovlaštenoj uporabi - puške postanu neprecizne, igrači se pretvore u ptice, itd.. [Bohemia Interactive's CEO on fighting piracy, creative DRM. URL: <https://www.pcgamer.com/interview-bohemia-interactives-ceo-on-fighting-piracy-creative-drm/> (10.03.2018.)]

Croteam, tvrtka koja je izdala "Serious Sam 3: BFE" u studenom 2011. godine, implementirala je malo drugačiji oblik zaštite. U igri se pojavi neuništivi lik koji konstantno napada igrača dok isti ne bude ubijen.

## SERIJSKI KLJUČEVI

Jedna od najstarijih i najmanje kompliciranih metoda zaštite DRM-a za računalne i Nintendo NES igre bila je da se igra zaustavi i zamoli da potražite određenu stranicu u knjižici koja se dobije sa igrom. Ako nemate tu knjigu - ne unesete ključ koji traži - niste mogli nastaviti igrati igru. Ključ proizvoda (engl. Serial Key), obično alfanumerički serijski broj koji se koristi za predstavljanje licence za određeni softver. Za vrijeme instalacije softvera ili po samom završetku instalacije kod pokretanja softvera, korisnika se traži da unese taj ključ. Tek nakon što ga unese, a on prođe provjeru i bude valjan, korisnik može koristiti proizvod.



Slika 8 Softver traži serijski broj kako bi nastavio sa instalacijom

Izvor: <https://i1.wp.com/www.techwd.net/wp-content/uploads/2017/10/How-to-Find-Serial-Key-Of-Any-Software.jpg?fit=800%2C622>

No pošto se softveri mogu „kreirati“ kako bi se koristili bez provjere ključa, te zbog toga što su stvoreni "keygen" programi koji bi mogli generirati ključeve automatski sve dok neki ne bude prihvaćen, obično se danas koriste u kombinaciji s online aktivacijom.



Slika 9 Primjer Keygen softvera

Izvor: <https://i0.wp.com/www.easycrack.net/wp-content/uploads/2015/04/universal-keygen-generator-2015-full-version-download.html>

#### 4.5. GLAZBA

U početku, zaštita glazbe na CD-ima nije bila najkompaktnija, te nije ispunjavala standarde. Stoga na tim CD-ima - na kojima se nije koristio Red Book standard već neka DRM shema - nije bilo logotipa CD. Također, nisu se mogli reproducirati ispravno na CD playerima ili računalima. Posebice na Windows sustavima, koji su se ponekad čak znali i srušiti prilikom pokušaja reprodukcije.

U 2005. godini Sony BMG predstavio je novu DRM shemu koja instalira softver na korisnikovo računalo bez da mu jasno da do znanja ili ga traži za dozvolu. Između

ostalog, instalirani softver uključivao je *rootkit*<sup>15</sup> koji je stvarao mogući sigurnosni propust te samim time ranjivost sustava na kojemu je instaliran. Naknadno, sve su te mane izašle u javnost, što dovodi do nezadovoljstva i brige korisnika. Sony BMG je pokušavao smanjiti sve te ranjivosti što je više moguće, no na kraju su morali povući na milione CD-ova, te su objavili nekoliko zakrpa koji su trebali u najmanju ruku ukloniti *rootkit*. Podignuto je nekoliko tužbi koje su riješene sporazumom, gdje su korisnicima ili vraćena uložena sredstva ili im je omogućeno besplatno skidanje albuma - koji nije koristio DRM.

Prije nekoliko godina dosta velika kontroverza izbila je kada je Mark Russinovich, poznati autor vrhunskih administratorskih alata iz serije SysInternals, otkrio da se na Windows instalira rootkit nakon što korisnik u uređaj računala ubaci CD i poželi ga slušati. Taj incident zanimljiv je iz nekoliko razloga, a najviše zato što instaliranje takvih programa otvara računalo za druge ranjivosti Protiv Sonyja pokrenute su neke tužbe, te su odustali od takve vrste špijuniranja. [Rootkit – špijun u vašem računalu URL: [pcchip.hr/softver/sigurnost/rootkit-spijun-vasem-racunalu](http://pcchip.hr/softver/sigurnost/rootkit-spijun-vasem-racunalu) (10.03.2018.)]

Sony BMG softver imao je ograničenu moć sprječavanja kopiranja jer je utecao samo na reprodukciju na Windows OS računalima, no ne i na drugim uređajima i opremi. Ali i uz to korisnici su pronašli put kako bi i na Windows OS zaobišli ograničenja. Držanjem tipke Shift za vrijeme umetanja CD-a ili jednostavno onemogućavanjem Autorun opcije. Osim toga, audio zapisi se jednostavno mogu reproducirati te ponovno snimiti čime se potpuno zaobilazi DRM. Taj propust poznat je pod nazivom "analogna rupa".

U siječnju 2007. EMI<sup>16</sup> je prestao sa izdavanjem DRM zaštićenih glazbenih CD-a jer su troškovi preveliki u odnosu na rezultate koje bi trebali ostvariti (odnosno nisu ostvareni). Popratio ih je i Sony BMG koji je bio zadnji od većih glazbenih izdavača,

---

<sup>15</sup> Rootkit je skupni naziv za vrstu programa koji su namijenjeni preuzimanju nadzora nad računalom ili nekim njegovim dijelovima a da pritom ostanu skriveni od pogleda korisnika, administratora ili programa za zaštitu.

Nije nužno da rootkit bude program s nekom zlom namjerom u konačnici, ali kako se sve uvijek voli zloupotrijebiti, tako su i programi iz reda rootkita na koncu upotrebljavani uglavnom za zlonamjerne aktivnosti.

<sup>16</sup> Electric and Musical Industries bio je britanski multinacionalni konglomerat osnovan u ožujku 1931. godine sa sjedištem u Londonu. U vrijeme raspada 2012. godine bila je četvrta najveća poslovna grupacija u glazbenoj industriji uz Universal Music Group, Sony Music Entertainment, te Warner Music Group.



koji je napustio DRM. Opće shvaćeno i opće prihvaćeno je kako nije urodilo plodom da se zaštite glazbeni CD-i sa DRM tehnologijama.

### **ZAŠTITA GLAZBE KOJA SE NALAZI NA INTERNETU**

Mnoge internetske glazbene trgovine koriste DRM za ograničavanje korištenja kupljene te preuzete glazbe. Prije 2009. godine Apple je počeo koristiti za svoju iTunes trgovinu FairPlay DRM sistem. Apple nije licencirao svoj DRM drugim tvrtkama, pa su samo Apple uređaji te Apple QuickTime mogli reproducirati glazbu s iTunes-a. U svibnju 2007. godine EMI pjesme su postale dostupne u iTunes Plus formatu, no i koštale su više. Te pjesme su bile veće kvalitete (256 kbit/s) te oslobođene DRM-a. No već nekoliko mjeseci kasnije cijene su bile znatno spuštene. Tek u Travnju 2009 sva iTunes glazba oslobođena je DRM-a. Video zapisi te iOS aplikacije nastavile su koristiti FairPlay politiku.

Servis iTunes omogućava korisnicima preuzimanje različitih digitalnih sadržaja poput glazbenih albuma, pojedinačnih pjesama, filmova, televizijskih serija, radijskih i drugih (podcast) emisija i sl. Budući da digitalna distribucija čini nepotrebnim skupo tiskanje podatkovnih medija i popratnih sadržaja, cijene sadržaja su relativno niske. Appleov sustav zaštite i upravljanja digitalnim sadržajima distribuiranim preko iTunes dućana naziva se Apple Fairplay.

U tehničkom smislu, sadržaj kupljen preko iTunesa dostavlja se na korisnikovo računalo, mobitel, tablet računalo, digitalni kućni medijski centar ili drugi uređaj u DRM šifriranom obliku. Pri tome se upotrebljava tzv. Advanced Audio Coding – AAC algoritam pohrane digitalnih medijskih podataka, za koji Apple tvrdi da je efikasniji i kvalitetniji od široko rasprostranjenog MP3 formata. Prije pristupa sadržaju korisnik je dužan pristati na uvjete ugovora o uvjetima usluge koji, među ostalim, ograničavaju broj prijenosa kupljenog sadržaja na podatkovni medij, broj autoriziranih uređaja koje korisnik može upotrebljavati za reprodukciju sadržaja, korisnikov pristanak na enkripciju sadržaja kako bi se spriječila neovlaštena upotreba sadržaja, te najvažnije – pristanak na mogućnost da Apple ograniči ili ukine pristup licenciranim sadržajima u slučaju da iz bilo kojeg razloga odluči ugasiti servis iTunes.

Napster glazbena trgovina nudi pristup temeljen na pretplati, kako bi korisnici obavili trajnu kupnje glazbenih sadržaja. Korisnici pretplatničke usluge mogu preuzeti i prenijeti neograničenu količinu glazbe u WMA (Windows Media Audio) formatu. Po

isteku pretplate sva kupljena glazba postaje nedostupna dok korisnik ne produži svoju pretplatu. Napster dodatno naplaćuje korisnicima ako žele koristiti glazbu na prijenosnim uređajima te ako žele snimiti glazbu na CD. Glazba kupljena putem Napstera može se reproducirati na softveru koji nosi Microsoft PlaysForSure logo. No od lipnja 2009. Napster nudi i DRM free verziju koja se može reproducirati i na iPhone te iPod uređajima.

Online trgovina glazbom, „Wal-Mart Music Downloads“ omogućuje reprodukciju na bilo kojem Windows PlaysForSure uređaju. No problem je da se glazba morala kopirati u internu pohranu Sansa – uređaja za reprodukciju mp3 sadržaja. Ako bi se sadržaj kopiralo na microSD karticu, reprodukcija ne bi bila moguća.

Sony je upravljao "Connect" uslugom za preuzimanje glazbe, koja je koristila Sonyjevu OpenMG DRM tehnologiju. Glazba oduzeta putem ove trgovine mogla se je reproducirati samo na računalima koja koriste Microsoft Windows i hardver tvrtke Sony (uključujući PSP i još neke Sony Ericsson mobitele).

Kazaa je jedna od rijetkih usluga koje nude model određivanja cijena na temelju pretplate, Međutim, preuzimanja glazbe s internetske stranice Kazaa su zaštićene DRM-om tako da se mogu reproducirati samo na računalima i prijenosnim uređajima s programom Windows Media Player, dokle god je klijent pretplaćen na Kazaa.

#### 4.6. SERVISI ZA STRUJANJE MULTIMEDIJKOG SADRŽAJA

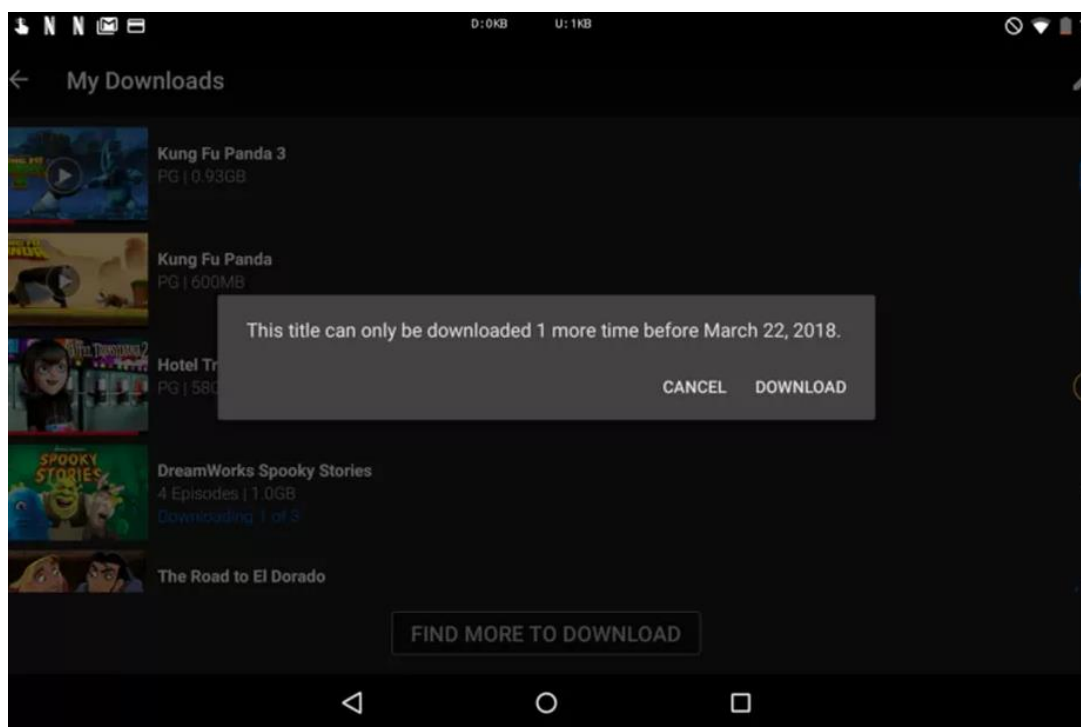
S početkom 21. stoljeća trend je postao iznajmljivanje medija putem servisa za strujanje (engl. Streaming Services) istih. Primjer su usuge Spotify za glazbu, te Netflix za video sadržaj. Nositelji autorskih orava zahtijevaju da te usluge štite sadržaj putem DRM mehanizma.

Spotify je streaming servis koji postavlja DRM u svojoj kolekciji glazbe - koristi ga kao sredstvo za zaštitu protiv piratstva - što stvara korisnicima probleme još od pokretanja ovog servisa. Sprečavanje djeljenja skinute pjesme, iako je kupljena od strane pretplatnika, te nemogućnost slušanja na bilo kojem drugom uređaju ili softveru, sem samog Spotify-a, razlog je nezadovoljstva. No kako je poznato, svaki problem ima i rješenje, pa tako i ovaj. Razvijeni su softveri, koji omogućuju zaobilaznje DRM-a, te

skidanje glazbe (u nekoliko standardnih formata) kako bi ju korisnici mogli slobodno koristiti. Jedan od njih, najpopularniji je Sidify.

Netflix je odličan primjer za multi-DRM solucije. Ovisno o uređaju preko kojega se koristi služi se drugom DRM metodom. Uglavnom koristi Playready DRM (Silverlight/Playstation/Wii) te nešto manje Widevine i HTML5/EME (Safari/Chrome).

Krajem 2016. Netflix je omogućio preuzimanja za offline reprodukciju, što je bila dobra vijest za pretplatnike koji putuju avionom, podzemnom, ili se jednostavno nađu na mjestu ili u situaciji bez pristupa internetu. No i tu nije bilo sve savršeno, jer su ugradili naredbe za suspendiranje sadržaja poput datuma isteka skinutog sadržaja, te ograničene podrške za pohranu na microSD - kartici za pohranu digitalnog sadržaja - na Android uređajima. Prikazano na slici 10, naknadno je ograničen i broj mogućih skidanja sadržaja u jednoj godini.



Slika 10 Netflix-ovo ograničenje

Izvor: <https://www.androidpolice.com/2017/06/13/lame-netflix-places-limits-many-times-can-download-certain-content/>

## ZAKLJUČAK

Gotovo istog trenutka kada su digitalni mediji „ušli“ u modu, vidjeli smo pokušaje da se filmove, igre, glazbene spotove, itd. zaštiti od neovlaštenog dijeljenja i aktivnosti koje spadaju pod piratstvo. Vlasnici i autori su stavljali kao zaštitu upozorenja. Na primjer prije početka filma, umetnuli bi sliku na kojoj piše nešto tipa da je bilo kakva neovlaštena reprodukcija i distribucija ilegalna, te da će svako kršenje navedenog biti kažnjavano na ovakav ili onakav način. Nije tajna da ti isti vlasnici i kompanije koje proizvode sadržaj, gledaju na one koji neovlašteno barataju njima, kao ozbiljan problem. Ne tako davno prestali su nas „samo“ upućivati na ispravno korištenje, i odlučili korisnike ograničiti na ono što mogu/smiju a što ne mogu/ ne smiju, implementiranjem tehnologije zvane DRM (Digital Rights Management).

Najranija forma DRM-a se je osnivala na šifriranju i dešifriranju ključevima. Ukratko DVD čitači bi imali ugrađen ključ koji bi dešifrirao ono što je bilo prethodno šifrirano na DVD disku. Problem koji se ovdje pojavio je taj da je samo bilo pitanje vremena kada će netko provaliti koji je ključ te ga iskoristiti na neprimjeren način.

Imamo još mnogo stvari na raspolaganju u DRM-ovu „arsenalu“, a jedno od njih, s kojim bi trebali biti upoznati ako kupujete muziku s iTunesa ili igrice putem Steam-a, jest online autentifikacija (nedvosmislena identifikacija korisnika). Mnogo igrica i programa kontroliraju način na koji su korišteni, vezivanjem kupnje istih uz specifičan račun (npr. korisnički račun na Originu ili Steam-u), te zahtijevaju od programa da provjerava da li su ili uređaj ili korisnički račun putem kojega su spojeni na poslužitelja, prošli autentifikaciju. Tek nakon autentifikacije, medij se, u ovom slučaju igrica, može putem poslužitelja igrati na tome uređaju/računalu.

Mnoge usluge poput Spotify i Netflix-a koriste neku formu DRM-a kako bi spriječili ljude od preuzimanja i korištenja multimedijalnih datoteka, a da nisu pretplaćeni na tu uslugu. Neki su pronašli alternative za doći do željenog sadržaja no mnogi ne nude, odnosno rijetki su oni, koji nude taj sadržaj na istoj razini i kvalitetan poput originala. Najbolji primjer su piratske verzije novih, tek predstavljenih filmova koji se puštaju u kinima, a netko ih u kinu snima kamerom (snima platno) i onda prenese na Internet kako bi dijelio sa drugima. Tada te verzije obično u svom nazivu imaju i sufikse poput: 'CAM', 'CAMRip' ili 'HD-CAM'.

Naravno tu su i dalje fizički mediji. Blu Ray i DVD, koji su uglavnom zastali na šifriranju i dešifriranju putem ključeva poštu su namijenjeni reproduciranju putem medija/uređaja koji nemaju vezu s internetom. No postoje sheme poput regionalnog zaključavanja (engl. Region locking) koja je u uporabi već duže vremena, a sprječava reprodukciju diska tj. njegovog sadržaja u drugim regijama/državama. Kada bi se na primjer u Rusiji kopirali filmovi iz videoteke, te kopije se ne bi mogle reproducirati na uređajima u SAD-u.

Ljudi, u naravi, ne vole kada im netko govori što smiju, a što ne smiju činiti sa stvarima koje su kupili. Iz toga je i nastala velika rasprava oko toga koliko je DRM prigodan, te je nastala borba između hakera koji zaobilaze zaštite, te multimedijalnih kompanija koje pokušavaju razviti što bolje verzije šifriranja sadržaja kako bi zaštitili svoje sadržaje. Pola zasluga za ovaj pokret nosi famozni zakon – DMCA (Digital Millennium Copyright Act), po kojemu su sve navedene neovlaštene radnje - koje krše pravila DRM-a - nezakonite te se za njih snose posljedice. Postale su nedopuštene i radnje koje nisu dio navedenih spornih radnji, kao kopiranja sadržaja u vlastite, sigurnosne svrhe, poput sigurnosne kopije u slučaju požara i sličnih ekstremnih i manje ekstremnih uvjeta.

Sa druge strane vlasnici tih sadržaja su zagovarali kako bi dostupnost istih bez utjecaja DRM-a dovelo do masovnog piratstva i doba gdje bi ljudi putem Torrent-a mogli skinuti cijelu sezonu Hello Kitty animirane serije u samo nekoliko minuta.

Tko je u pravu, korisnici koji kupe taj sadržaj i tada misle da mogu raditi što žele s njim ili distributeri i intelektualni vlasnici tih sadržaja koji pokušavaju što bolje zaštititi svoja prava? Kako sve više i više sadržaja postaje digitalno nema sumnje da nove tehnologije uz nove politike pokušavaju pronaći savršeni balans. Sve dok se taj savršeni balans ne postigne, sigurno je da će stalno biti na kušnji.

## LITERATURA

Državni zavod za intelektualno vlasništvo. URL: <http://www.dziv.hr/hr/intelektualno-vlasnistvo/o-intelektualnom-vlasnistvu/> (26.02.2018.)

Genius Croatia, baza ideja, izuma i inovacija iz Hrvatske, URL: <http://genius-croatia.com/info/pitanja-i-odgovori/> (26.02. 2018.)

Van Tassel, J. (2016.) Digital Rights Management: Protecting and Monetizing Content. Focal Press

The pros, cons, and future of DRM, URL: <http://www.cbc.ca/news/technology/the-pros-cons-and-future-of-drm-1.785237> (27.02.2018.)

The Statute of Anne, 1710. URL: <https://www.copyrighthistory.com/anne.html> (27.03.2018.)

Expression Language And Guides The Copyright Holder, URL: <https://www.coursehero.com/file/p4tc8ev/expression-language-and-guides-the-copyright-holder-through-the-process-of/> (27.02.2018.)

RipGuard copy protection - process, URL: <http://www.hellmanproduction.com/cd/dvd-replication/ripguard-copy-protection-process.html> (10.03.2018.)

How Digital Rights Management Works, URL: <https://computer.howstuffworks.com/drm2.htm> (27.02.2018.)

Dragičević D., Katulić, T. (2013.) Utjecaj DRM tehnologija na tržište digitalnih sadržaja

DRM Security Products, URL: [https://www.locklizard.com/digital\\_rights\\_management\\_products/](https://www.locklizard.com/digital_rights_management_products/) (11.03.2018.)

Drumlin Security, URL: <https://www.drumlinsecurity.com/> (20.01.2018.)

AACS – Sustav za zaštitu digitalnog sadržaja, URL: <https://www.cis.hr/files/dokumenti/CIS-DOC-2011-02-003.pdf> (10.03.2018.)

What is AACS, URL: <https://www.aacsla.com/what/overview> (11.03.2018.)

Programmi, film e serie tv on demand, URL: <http://www.tivuon.tv/cosa-e-tivuon.aspx> (11.03.2018.)

Amazon Erases Orwell Books From Kindle Devices. New York Times URL: <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html> (11.03.2018.)

Top 10 Most Pirated Games of 2008, URL: <https://torrentfreak.com/top-10-most-pirated-games-of-2008-081204> (10.03.2018.)

Ubisoft undone by anti-DRM DDoS storm. URL: [https://www.theregister.co.uk/2010/03/08/ubisoft\\_anti\\_drm\\_hack\\_attack](https://www.theregister.co.uk/2010/03/08/ubisoft_anti_drm_hack_attack) (27.02.2018.)

Bohemia Interactive's CEO on fighting piracy, creative DRM. URL: <https://www.pcgamer.com/interview-bohemia-interactives-ceo-on-fighting-piracy-creative-drm/> (10.03.2018.)

Rootkit – špijun u vašem računalu URL: [pcchip.hr/softver/sigurnost/rootkit-spijun-vasem-racunalu](http://pcchip.hr/softver/sigurnost/rootkit-spijun-vasem-racunalu) (10.03.2018.)

Digitalni Vodeni žigovi, URL: <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-08-310.pdf> (28.12.2017.)

Metadata at W3C. URL: <https://www.w3.org/Metadata/> (10.03.2018.)

Subramanya, S.R. & Yi, B.K.. (2006). Digital rights management.

Digital Rights Management, URL: [https://www.researchgate.net/publication/3227866\\_Digital\\_rights\\_management](https://www.researchgate.net/publication/3227866_Digital_rights_management) (30.11.2017.)]